

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-056963

(43)Date of publication of application : 25.02.2000

(51)Int.Cl.

G06F 9/06
G06F 12/14
G06K 19/073

(21)Application number : 10-235034

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 06.08.1998

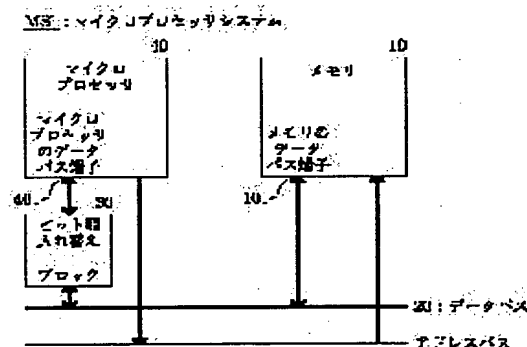
(72)Inventor : URANO MASAMI

(54) MICRO PROCESSOR SYSTEM, MICRO PROCESSOR OPERATION ANALYSIS PREVENTING METHOD, AND RECORDING MEDIUM RECORDED WITH MICRO PROCESSOR OPERATION ANALYSIS PREVENTING PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a micro processor system by which the analysis of a program on a memory and a bus is difficult so that the operation of the micro processor is not analyzed even if the program is read, and to provide a micro processor operation analysis preventing method and a recording medium in which a micro processor operation analysis preventing program is recorded.

SOLUTION: This system is constituted of a micro processor 40, a memory 10 preserving at least a program or data which can be executed by the micro processor 40, and address bus/data bus 20 connecting the micro processor 40 to the memory 10. The bit order of the terminal of the data bus 20 of the micro processor 40 and the bit order of the terminal of the data bus 20 of the memory 10 are changed.



LEGAL STATUS

[Date of request for examination] 22.01.2001

[Date of sending the examiner's decision of rejection] 21.05.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-56963

(P2000-56963A)

(43) 公開日 平成12年2月25日 (2000.2.25)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 9/06	5 5 0	C 0 6 F 9/06	5 5 0 B 5 B 0 1 7
12/14	3 2 0	12/14	3 2 0 B 5 B 0 3 5
G 0 6 K 19/073		G 0 6 K 19/00	P 5 B 0 7 6

審査請求 未請求 請求項の数12 F D (全 15 頁)

(21) 出願番号 特願平10-235034

(22) 出願日 平成10年8月6日 (1998.8.6)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 浦野 正美

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内

(74) 代理人 10008/446

弁理士 川久保 新一

Fターム(参考) 5B017 AA07 BA07 CA04

5B035 AA13 BB09 CA38

5B076 FA02

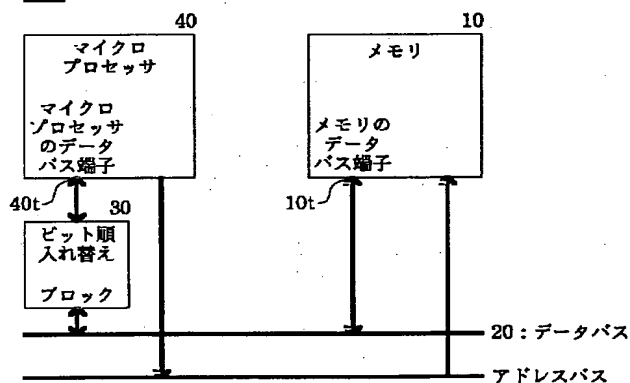
(54) 【発明の名称】 マイクロプロセッサシステム、マイクロプロセッサ動作解析防止方法およびマイクロプロセッサ動作解析防止プログラムを記録した記録媒体

(57) 【要約】

【課題】 プログラムを読み取られても、マイクロプロセッサの動作を解析されないように、メモリ上およびバス上のプログラムの解析が困難であるマイクロプロセッサシステム、マイクロプロセッサ動作解析防止方法およびマイクロプロセッサ動作解析防止プログラムを記録した記録媒体を提供するものである。

【解決手段】 マイクロプロセッサと、上記マイクロプロセッサで実行可能なプログラム、データのうちの少なくとも一方を保存するメモリと、上記マイクロプロセッサと上記メモリとを接続するアドレスバスとデータバスとによって構成されているシステムにおいて、上記マイクロプロセッサのデータバスの端子のビット順と上記メモリのデータバスの端子のビット順とを変えるものである。

MS1: マイクロプロセッサシステム



【特許請求の範囲】

【請求項1】 マイクロプロセッサと、上記マイクロプロセッサで実行可能なプログラム、データのうちの少なくとも一方を保存するメモリと、上記マイクロプロセッサと上記メモリとを接続するアドレスバスとデータバスとによって構成されているマイクロプロセッサシステムにおいて、

上記マイクロプロセッサが処理する上記データまたは上記プログラムのビット順と、上記メモリに格納されている上記データまたは上記プログラムのビット順とを異ならせることを特徴とするマイクロプロセッサ動作解析防止方法。

【請求項2】 請求項1において、上記メモリに格納されている上記データまたは上記プログラムの同一ワード内におけるビット順を入れ換えることによって、上記マイクロプロセッサが処理する上記データまたは上記プログラムのビット順と同一になることを特徴とするマイクロプロセッサ動作解析防止方法。

【請求項3】 請求項1において、上記マイクロプロセッサに接続されている第1のメタル配線と、上記メモリに接続されている第2のメタル配線と、上記第1のメタル配線と上記第2のメタル配線との相互間に接続されているMOSトランジスタと、上記MOSトランジスタのゲートを制御する制御手段とによってビット順入れ換えブロックが構成され、上記MOSトランジスタのゲートに所望の制御信号を与えることによって、ビット順を入れ換えることを特徴とするマイクロプロセッサ動作解析防止方法。

【請求項4】 請求項1において、上記メモリのデータバス端子と上記マイクロプロセッサのデータバス端子との接続順に基づいて、上記マイクロプロセッサのプログラムの各ワード内のビット順を変更することを特徴とするマイクロプロセッサ動作解析防止方法。

【請求項5】 ビット順変換前のデータまたはプログラムを所定バイト、読み込む読み込み手順と；上記読み込んだ所定バイトの中でビット位置の入れ換えを行うビット位置入れ換え手順と；上記ビット位置の入れ換えが行われたデータまたはプログラムを書き出す書き出し手順と；をコンピュータに実行させるマイクロプロセッサ動作解析防止プログラムが記録されているコンピュータ読み取り可能な記録媒体。

【請求項6】 マイクロプロセッサと、上記マイクロプロセッサで実行可能なプログラム、データのうちの少なくとも一方を保存するメモリと、上記マイクロプロセッサと上記メモリとを接続するアドレスバスとデータバスとによって構成されているマイクロプロセッサシステムにおいて、

上記マイクロプロセッサが処理するプログラム、データのうちの少なくとも一方のビット順と、上記メモリに格

納されているプログラム、データのうちの少なくとも一方のビット順とを異ならせるビット順入れ換えブロックを有することを特徴とするマイクロプロセッサシステム。

【請求項7】 請求項6において、上記ビット順入れ換えブロックは、上記マイクロプロセッサのデータバス端子と上記データバスとの間の領域、または、マイクロプロセッサコアとマイクロプロセッサのデータバス端子との間の領域に設けられていることを特徴とするマイクロプロセッサシステム。

【請求項8】 請求項6において、上記メモリは、上記ビット順入れ換えブロックによって、ワード内のビットが入れ換えられたプログラム、データのうちの少なくとも一方を格納するメモリであることを特徴とするマイクロプロセッサシステム。

【請求項9】 請求項6において、上記ビット順入れ換えブロックは、上記マイクロプロセッサに接続されている第1のメタル配線と；上記メモリに接続されている第2のメタル配線と；上記第1のメタル配線の所定部分と上記第2のメタル配線の所定部分とを接続するスルーホールと；を有するブロックであることを特徴とするマイクロプロセッサシステム。

【請求項10】 請求項6において、上記ビット順入れ換えブロックは、上記マイクロプロセッサに接続されている第1のメタル配線と；上記メモリに接続されている第2のメタル配線と；上記第1のメタル配線と上記第2のメタル配線との相互間に接続されているMOSトランジスタと；上記MOSトランジスタのゲートを制御する制御手段と；を有し、上記MOSトランジスタのゲートに所望の制御信号を与えることによって、ビット順を入れ換えるブロックであることを特徴とするマイクロプロセッサシステム。

【請求項11】 請求項10において、上記制御信号は、上記メモリの所定のワード内の所定のビットに格納されていることを特徴とするマイクロプロセッサシステム。

【請求項12】 請求項6において、上記メモリに格納されているプログラムまたはデータは、同一ワード内のビット順を入れ換えることができるプログラムによって生成されたものか、または上記ビット順を入れ換えることができる機能を持つプログラムによって、上記メモリ上にロードされているものであることを特徴とするマイクロプロセッサシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ICカード等に用いるマイクロプロセッサに関するものである。

【0002】

【従来の技術】図19は、従来のマイクロプロセッサシ

システムMSの構成の一例を示す図である。

【0003】ここでは、8ビットのマイクロプロセッサであるZ80を例にとって説明するが、さらに多ビットのマイクロプロセッサを使用した場合も、上記の場合と同様に考えることができる。

【0004】従来のマイクロプロセッサシステムMSは、マイクロプロセッサ4とメモリ1とによって構成され、マイクロプロセッサ4のアドレスバス端子とメモリ1のアドレスバス端子とがアドレスバスによって接続され、マイクロプロセッサ4のデータバス端子4とメモリ1のデータバス端子1とがデータバス2によって接続されている。

【0005】図20は、上記従来例におけるマイクロプロセッサのデータバス端子とメモリのデータバス端子との接続を示す図である。

【0006】上記従来例において、マイクロプロセッサ4側のデータバス2のMSBの配線D7とメモリ1側のデータバスのMSBの配線D7とが接続されている。配線D6、D5、…D0のそれぞれも、上記と同様に、同じビット順同士が接続されている。

【0007】図21は、従来例におけるメモリ1の内容を示す図である。

【0008】マイクロプロセッサ4が実行するプログラムは、図21に示すように、メモリ1中に保存され、ここでは、8ビットマイクロプロセッサ4であるZ80を例にとって説明するが、他のマイクロプロセッサでも、上記と同様である。

【0009】ここに示した例では、0番地に16進数で31（以下、16進数で示す）（00110001）、1番地にFF、2番地に7F、3番地に06等が格納されている。また、4番地以降にも、上記と同様に、プログラムが格納されている。これらは、Z80の機械語では、LD SP, 7FFF、LD B, 11等を示している。

【0010】マイクロプロセッサ4がリセット信号によりリセットされ、次にリセットが解除されると、マイクロプロセッサ4はアドレスバスに0を出力する。このデータをアドレスとして、メモリ1がその0番地の内容31をデータバス2に出力すると、マイクロプロセッサ4は、そのデータを内部に取り込んでデコードし、さらにオペランドを取得するために、1、2をアドレスバスに出力し、それぞれの番地の内容のFF、7Fをメモリ1から読み出す。

【0011】マイクロプロセッサ4は、これらの読み出されたデータをLD SP, 7FFFという命令であると解釈し、自分自身のSPに7FFFを設定する。その後、次の命令を取得するために、4をアドレスバスに出力し、メモリ1の4番地の内容の06を読み出す。以上のようにして、マイクロプロセッサ4は順次アドレスを出力し、メモリ1の該当する番地の内容を読み出して命

令を実行していく。

【0012】上記のように、従来のマイクロプロセッサ4では、データバス2を介して、メモリ1の内容を順次読み出し、その値をマイクロプロセッサ4内部で解釈し、そのデータに対応する命令を順次実行する。プログラム自体は、実行する順番で、メモリ1上に格納されている。また、各番地には、プログラムの各ステップの命令コードが格納され、メモリ1のMSB側（ここではビット7とする）に命令コードのMSB（ビット7）が格納され、メモリ1のビット6には命令コードのビット6が格納され、同様に、LSBまで順番に格納されている。

【0013】ところで、近年ICカードの応用分野が拡大しつつあるが、これにつれてICカードのセキュリティの問題が重視されている。ICカード内に納められている機密情報を解読しようとする場合、マイクロプロセッサ4の論理回路、プログラムを容易に解読することができると、この情報を元に内部を解析し、機密情報を解読される可能性がある。

【0014】

【発明が解決しようとする課題】従来のマイクロプロセッサ4のように、プログラムがメモリ1上に順番に、かつ各ワード内でもビット順に格納されている場合、該当するメモリセルのデータを順番に読み取ることによってプログラムが容易に解読される可能性がある。

【0015】また、上記のように、プログラムはメモリ1からデータバス2を介してマイクロプロセッサ4に送られ、この場合、メモリ1のデータを解析しなくても、データバス2を観測することによって、プログラムを順次読み取ることができ、これをもとに動作を容易に解析される可能性がある。

【0016】本発明は、プログラムを読み取られても、マイクロプロセッサの動作を解析されないように、メモリ上およびバス上のプログラムの解析が困難であるマイクロプロセッサシステム、マイクロプロセッサ動作解析防止方法およびマイクロプロセッサ動作解析防止プログラムを記録した記録媒体を提供するものである。

【0017】

【課題を解決するための手段】本発明は、マイクロプロセッサと、上記マイクロプロセッサで実行可能なプログラム、データのうちの少なくとも一方を保存するメモリと、上記マイクロプロセッサと上記メモリとを接続するアドレスバスとデータバスとによって構成されているシステムにおいて、上記マイクロプロセッサのデータバスの端子のビット順と上記メモリのデータバスの端子のビット順とを変えるものである。

【0018】

【発明の実施の形態および実施例】図1は、本発明の第1の実施例であるマイクロプロセッサシステムMS1を示す図である。

【0019】マイクロプロセッサシステムMS1は、基本的には、従来例と同様のシステムであるが、データバス20とマイクロプロセッサ40のデータバス端子40ととの間に、ビット順入れ換えブロック30が接続されている点が、上記従来例とは異なる。

【0020】メモリ10側において、データバス20の各ビットが、従来例と同様に、メモリ10のデータバス端子10との同じビットに順番に接続されている。また、マイクロプロセッサ40のアドレスバスの端子におけるビット順と、メモリ10のアドレスバスの端子におけるビット順とは、同じ順序で接続されている。つまり、アドレスに関して、ビット順入れ換えブロックが設けられていない。

【0021】図2は、上記実施例におけるビット順入れ換えブロック30の具体例を示す図である。

【0022】図2に示す例では、ビット順入れ換えブロック30によって、マイクロプロセッサ40のデータバス端子40側の配線D7をメモリ10のデータバス端子10側の配線D5へ入れ換え、以下それぞれ、D6をD2へ、D5をD1へ、D4をD6へ、D3をD0へ、D2をD4へ、D1をD3へ、D0をD7へ入れ換えて接続している。

【0023】なお、図2では、1種類の接続法が記載されているが、データバス20の各ビットと、マイクロプロセッサ40のデータバス端子40との各ビットとを、1:1に接続するものであれば、図2に示すブロック30における接続法以外の接続法を採用するようにしてもよい。

【0024】図3は、上記実施例におけるメモリ10に格納すべきデータの例を示す図である。

【0025】上記実施例では、メモリ10のデータバス端子10のビット順と、マイクロプロセッサ40のデータバス端子40のビット順とが互いに異なるので、従来と同様の命令コードをメモリ10に格納しても、マイクロプロセッサ40が正常には動作しない。

【0026】つまり、メモリ10の0番地に、従来例と同様に、たとえば、31(00100001)を格納しても、ビット順入れ換えブロック30によって、データが入れ換えられ、マイクロプロセッサ40のデータバス端子40では8C(10001000)になり、マイクロプロセッサ40は、これをADC A、Hという命令と解釈する。したがって、正常に動作させるためには、命令コードのビット順を予め入れ換えた後に、メモリ10に格納する必要がある。この場合、0番地にデータC2を格納し、1番地にデータFFを格納し、2番地にデータDFを格納し、以下各番地に、データ18、C0、19、0A、88、B4、F4を格納する。

【0027】図4は、メモリ10のデータバス端子10におけるプログラムのビット順と、マイクロプロセッサ40のデータバス端子40におけるプログラムのビ

ット順とが、どのように変換されているかを具体的に示す図である。

【0028】メモリ10のデータバス端子10に、0番地のデータとして、10000010(C2)のデータが出力されたとすると、各ビットはビット順入れ換えブロック30を介して、マイクロプロセッサ40のデータバス端子40に到達し、その値はビット7から順番に00100001(31)になり、LD SP, nn(nnは16bitの値)という命令であり、この命令コードは、従来例における命令コードと同じ命令コードである。

【0029】ここで、まず、元となるプログラムにおける各ワード内のビット順を予め入れ換え、このようにビット順を入れ換えたデータを、メモリ10に格納しておく。マイクロプロセッサ40が、従来例と同様に各番地のデータを順次読み出し、このデータ読み出し時に、メモリ10のデータバス端子10や、データバス20に出現するデータのビット順は、元のプログラムのビット順とは入れ替わっているので、データバス20に出現するデータをマイクロプロセッサ40がそのまま実行しても、元のプログラムと同じ動作をすることはできない。

【0030】すなわち、第三者がメモリ10の内容や、データバス20の内容を何らかの方法で観測し、マイクロプロセッサ40の動作を解析しようとしても、メモリ10に格納されているデータや、データバス20上のデータは、そのビット順が入れ換えられたデータであり、元のプログラムのビット順とは異なっているので、元のプログラムの動作を解析することは困難である。

【0031】ところが、データバス20に出現するデータが、ビット順入れ換えブロック30を介して、マイクロプロセッサ40のデータバス端子40に到達すると、ビット順入れ換えブロック30で各ワード内のビット順が入れ換えられ、その後、マイクロプロセッサ40に到達するので、マイクロプロセッサ40のデータバス端子40では元のプログラムと同じビット順になる。したがって、マイクロプロセッサ40は元のプログラムと同じ動作を実行することができる。

【0032】図5は、上記実施例におけるビット順入れ換えブロック30の具体例を示す図である。

【0033】ビット順入れ換えブロック30は、1層メタル配線と2層メタル配線とを有し、1層メタル配線と2層メタル配線とが基板を挟んで配置されているブロックである。なお、図5において、1層メタル配線が水平に描かれ、2層メタル配線が垂直に描かれている。そして、データバス20の各配線が1層メタル配線に接続され、マイクロプロセッサ40のデータバス端子40に接続されている各配線が2層メタル配線に接続されている。

【0034】そして、1層メタル配線の配線D7は、データバス20の配線D7に接続され、1層メタル配線の

配線D6は、データバス20の配線D6に接続され、以下、上記と同様に配線D0まで接続されている。また、2層メタル配線の配線D7は、マイクロプロセッサ40のデータバス端子40tの配線D7に接続され、2層メタル配線の配線D6は、マイクロプロセッサ40のデータバス端子40tの配線D6に接続され、以下、上記と同様に配線D0まで接続されている。

【0035】そして、1層メタル配線と2層メタル配線とが絶縁性の基板を挟んで重なる場所のうちで、所定の場所にスルーホールを設け、このスルーホールによって1層メタル配線と2層メタル配線とが接続され、これによって、ビット順入れ換えを行う。

【0036】つまり、ビット順入れ換えブロック30において、2層メタル配線の配線D7と1層メタル配線の配線D5とが接続され、2層メタル配線の配線D6と1層メタル配線の配線D2とが接続され、2層メタル配線の配線D5と1層メタル配線の配線D1とが接続され、2層メタル配線の配線D4と1層メタル配線の配線D6とが接続され、2層メタル配線の配線D3と1層メタル配線の配線D0とが接続され、2層メタル配線の配線D2と1層メタル配線の配線D4とが接続され、2層メタル配線の配線D1と1層メタル配線の配線D3とが接続され、2層メタル配線の配線D0と1層メタル配線の配線D7とが接続されている。

【0037】このように接続することによって、図4に示すビット順入れ換えブロック30と同様なビット順の入れ換えが行われる。

【0038】すなわち、ビット順入れ換えブロック30は、マイクロプロセッサ40に接続されている第1のメタル配線と、メモリ10に接続されている第2のメタル配線と、上記第1のメタル配線の所定部分と上記第2のメタル配線の所定部分とを接続するスルーホールとを有するブロックである。

【0039】なお、上記実施例は、1層メタル配線、2層メタル配線、1層メタル配線と2層メタル配線との間のスルーホールを用いた例であるが、これ以外の配線層を用いて、ビット毎に異なった配線を行うブロックを採用するようにしてもよい。

【0040】図6は、ビット順入れ換えブロック30の代わりに使用することができるビット順入れ換えブロック30aの構成を示す図である。

【0041】ビット順入れ換えブロック30aは、NチャネルMOSTランジスタによって、データバス20の配線の1つと、マイクロプロセッサ40のデータバス端子40tの配線の1つとを接続するブロックである。

【0042】つまり、図6に示す例では、マイクロプロセッサ40側の配線D7とデータバス20側の配線D7～D0のそれぞれとに、NチャネルMOSTランジスタのソースとドレインとが接続されている。マイクロプロセッサ40側の配線D6とデータバス20側の配線D7

～D0のそれぞれとに、上記と同様に、NチャネルMOSTランジスタが接続されている。配線D5～D0のそれぞれについても、上記と同様に、NチャネルMOSTランジスタが接続されている。

【0043】そして、上記NチャネルMOSTランジスタのうちの所定のNチャネルMOSTランジスタのゲート電極に0または1（制御信号）を印加する（すなわち、GNDまたはVDDに接続する）。これによって、マイクロプロセッサ40のデータバス端子40tとデータバス20との接続を行い、所定のビット順入れ換えを行う。

【0044】この場合、D0～D7に1を印加し（マイクロプロセッサ40側の配線D0とデータバス20側の配線D7とを接続するNチャネルMOSTランジスタのゲート電極に1を印加し）、またD4～D6、D7～D5、D2～D4、D1～D3、D6～D2、D5～D1、D3～D0にも1を印加し（VDDに接続し）、その他に、0を印加する（GNDに接続する）。これによって、図4に示すビット順入れ換えブロック30と同じビット順の入れ換えを行うことができる。

【0045】つまり、ビット順入れ換えブロック30aは、マイクロプロセッサに接続されている第1のメタル配線と、上記メモリに接続されている第2のメタル配線と、上記第1のメタル配線と上記第2のメタル配線との相互間に接続されているMOSTランジスタと、上記MOSTランジスタのゲートを制御する制御手段とを有し、上記MOSTランジスタのゲートに所望の制御信号を与えることによって、ビット順を入れ換えるビット順入れ換えブロックの例である。

【0046】なお、ビット順入れ換えブロック30aでは、NチャネルMOSTランジスタを使用しているが、NチャネルMOSTランジスタの代わりにPチャネルMOSTランジスタを使用し、ゲートに印加する信号（制御信号）の1と0とを反転させるようにしてもよく、これによって、ビット順入れ換えブロック30aにおける動作と同様の動作を実現することができる。

【0047】さらに、PチャネルMOSTランジスタとNチャネルMOSTランジスタとの両者を用いて、データバス20の配線の1つと、マイクロプロセッサ40のデータバス端子40tの1つの配線とを接続し、PチャネルMOSTランジスタのゲートには、NチャネルMOSTランジスタのゲートに印加する制御信号の反転信号を印加してもよく、これによっても、ビット順入れ換えブロック30aにおける動作と同様の動作を実現することができる。

【0048】また、ビット順入れ換えブロック30aに使用されている各MOSTランジスタの制御信号を、メモリ10の所定領域に格納するようにしてもよい。

【0049】図7は、ビット順入れ換えブロック30aに使用されている各MOSTランジスタの制御信号が、

メモリ10に格納されている例を示す図である。

【0050】メモリ10の0番地のビット7には、7-0の制御信号（マイクロプロセッサ40側の配線D7とデータバス20側の配線D0との断続を制御する制御信号）が格納され、ビット6には6-0の制御信号（マイクロプロセッサ40側の配線D6とデータバス20側の配線D0との断続を制御する制御信号）が格納され、以下、上記と同様にして、64ビットの制御信号が、メモリ10の0番地から7番地に格納されている。

【0051】図8は、図2に示したビット順の入れ換えをするために、ビット順入れ換えブロック30aに供給する制御信号を示す図である。

【0052】上記制御信号は、メモリ10の0番地から7番地に格納されているデータであり、その0番地から順に、00001000、00100000、01000000、00000010、00000100、10000000、00010000、00000001が格納されている。

【0053】図9は、図7に示すトランジスタの制御信号を使用して、ビット順入れ換えブロック30aを制御する場合に必要なメモリセルMCの具体例と、メモリセルMCとトランジスタとの接続関係を示す図である。

【0054】メモリ10の各ビット内の所定のノードと、対応するトランジスタのゲート電極とを接続することによって、所定のトランジスタをオンさせ、ビット順の入れ換えを可能にする。なお、ここでは、メモリセルMCとして1ポートのSRAMを示してあるが、1ポートのSRAMの代わりに、2ポートSRAM、EEPROM、ROM等を使用してもよく、このようにしても、1ポートのSRAMを使用した場合の効果と同様の効果を得ることができる。また、特にSRAMを使用し、そのSRAMに書き込むデータを変更すればビット順の入れ換えが可能であるので、所定の時点で、上記SRAMに書き込まれているデータを書き換えることによって、ビット順の入れ換えの順番を変更することも可能である。

【0055】図10は、上記実施例において、メモリ10に格納されるビット順変換プログラムの作成法の一例を示す図である。

【0056】プログラムP1は、従来のマイクロプロセッサ40で動作可能なプログラムであり、プログラムP2は、上記実施例におけるマイクロプロセッサ40で動作可能なプログラムであり、プログラムPは、プログラムP1をプログラムP2に変換するビット順変換プログラムである。つまり、同一ワード内のビット位置を変換するビット順変換プログラムPによって、元のプログラムP1からプログラムP2を作成する。このビット順変換プログラムPを格納するマスクROM61を作成し、このマスクROM61をマイクロプロセッサ40と接続する。

【0057】また、ROMライタを用い、上記変換後のプログラムP2をEPROM62やEEPROM63に書き込み、これを上記実施例のマイクロプロセッサ40と接続するようにしてもよい。

【0058】さらに、上記変換後のプログラムP2を読み込めるローダープログラム、またはマイクロプロセッサ40で動作しているローダープログラムを使用し、上記変換後のプログラムP2をRAMに読み込めば、上記変換後のプログラムP2を実行することができる。さらに、ローダープログラムまたはモニタプログラムがビット順変換機能を備えたものであれば、元のプログラムP1を直接変換し、この変換後のプログラムP2をRAMにロードし、マイクロプロセッサ40で実行するようにしてもよい。

【0059】図11は、上記実施例において、ビット順変換プログラムPによるビット順変換動作を示すフローチャートである。

【0060】上記ビット順変換プログラムPは、所定の記録媒体に記録され、この記録されたビット順変換プログラムを、マイクロプロセッサ40とは異なるコンピュータで実行するものである。上記所定の記録媒体として、図10に示すマスクROM61、EPROM62、EEPROM63等と、図示しないFD、CD-ROM等との2種類が考えられる。

【0061】まず、ビット順変換前のプログラムである元のプログラムP1を1バイトを読み込み（S1）、読み込んだ1バイトの中でビット位置の入れ換えを行う。ここでは、図2に示すビット順入れ換えブロック30におけるビット順変換と同じ順で変換する場合を示してある（S2）。すなわち、ビット7のデータをビット5に変更し、ビット6のデータをビット2に変更し、ビット5のデータをビット1に変更し、ビット4のデータをビット6に変更し、ビット3のデータをビット0に変更し、ビット2のデータをビット4に変更し、ビット1のデータをビット3に変更し、ビット0のデータをビット7に変更し、これによって、新しいデータを1バイト作成する。次に、このデータを書き出し（S3）、ファイル全体の処理が終わっていないければ（S4）、さらに1バイトのデータについて、上記と同様の処理（S1～S3）を実行する。

【0062】上記実施例において、ビット順変換プログラムPの代わりに、ローダーまたはモニタプログラムを使用するようにしてもよい。

【0063】つまり、上記マスクROM61、EPROM62、EEPROM63等と、図示しないFD、CD-ROM等は、ビット順変換前のデータまたはプログラムを所定バイト、読み込む読み込み手順と、上記読み込んだ所定バイトの中でビット位置の入れ換えを行うビット位置入れ換え手順と、上記ビット位置の入れ換えが行われたデータまたはプログラムを書き出す書き出し手順

とをコンピュータに実行させるマイクロプロセッサ動作解析防止プログラムが記録されているコンピュータ読み取り可能な記録媒体の例である。

【0064】図12は、本発明の第2の実施例であるマイクロプロセッサシステムMS2を示す図である。

【0065】マイクロプロセッサシステムMS2は、メモリ10と、データバス20と、マイクロプロセッサ41とを有するものである。マイクロプロセッサ41は、マイクロプロセッサコア41cと、ビット順入れ換えブロック30とを有するものである。

【0066】第1の実施例であるマイクロプロセッサシステムMS1では、データバス20とマイクロプロセッサ40のデータバス端子40tとの間に、ビット順入れ換えブロック30を接続してあるが、マイクロプロセッサシステムMS2では、マイクロプロセッサ41内にビット順入れ換えブロック30を配置し、マイクロプロセッサコア41cとデータバス端子41tとの間でビット順が入れ換えられ、データバス端子10tとマイクロプロセッサ41のデータバス端子41tとは、同じビット順で1:1に接続されている。

【0067】図13は、マイクロプロセッサシステムMS2に使用されているビット順入れ換えブロック30の具体例を示す図である。

【0068】マイクロプロセッサコア41cのデータバス端子41cの配線D7は、ビット順入れ換えブロック30を介して、マイクロプロセッサ41のデータバス端子41tの配線D5に接続されている。

【0069】このデータバス端子41tの配線D5は、データバス20の配線D5を介して、メモリ10のデータバス端子10tの端子D5に接続されている。すなわち、マイクロプロセッサコア41cのデータバス端子41cの配線D7は、メモリ10の配線D5に接続されている。

【0070】上記と同様に、マイクロプロセッサコア41cの配線D6は、マイクロプロセッサ41のデータバス端子41tの配線D2に接続され、これはデータバス20の配線D2を介して、メモリ10のデータバス端子10tの配線D2に接続されている。また、上記と同様に、マイクロプロセッサコア41cの各端子が、メモリ10のデータバス端子10tの所定の端子に接続されている。

【0071】上記のようにすると、マイクロプロセッサコア41cのデータバス端子41cと、メモリ10のデータバス端子10tとの間で、図2に示す接続と同等の接続を実現することができる。また、マイクロプロセッサシステムMS2におけるビット順入れ換えブロック30として、図5に示すビット順入れ換えブロック30、図6に示すビット順入れ換えブロック30aを使用することができる。

【0072】図14は、従来のマイクロプロセッサの内

部におけるマイクロプロセッサコアと双方向バッファとを示す図である。

【0073】マイクロプロセッサ41では、マイクロプロセッサ41内部の論理回路とメモリとを有するマイクロプロセッサコア41cと、その端子を外と接続する入力バッファ、出力バッファ、双方向バッファ等とによって構成されている。図14では、説明に必要な双方向バッファのみを示してある。上記双方向バッファは、通常、トライステート出力バッファと入力バッファとで構成され、入力端子Iは、トライステート出力バッファを介して入出力端子IOに接続され、入出力端子IOは、入力バッファを介して出力端子Oに接続されている。また、制御端子IOCONTによって、トライステートバッファは、出力またはハイインピーダンス状態に制御されている。入力端子Iは、マイクロプロセッサコア41cのデータ出力端子に接続され、出力端子Oは、マイクロプロセッサコア41cのデータ入力端子に接続され、入出力端子IOは、マイクロプロセッサ41のデータバス端子41tに接続されている。

【0074】図15は、図14に示すマイクロプロセッサ41において、図13に示す実施例を実現する具体的な回路を示す図である。

【0075】図15では、双方向バッファとマイクロプロセッサ41のデータバス端子41tとの間に、ビット順入れ換えブロック30を置いたものである。

【0076】図16は、図14に示すマイクロプロセッサ41において、図13に示す実施例を実現する別の具体的な回路を示す図である。

【0077】図16では、双方向バッファとマイクロプロセッサコア41cとの間に、ビット順入れ換えブロック30を置いたものである。

【0078】図15、図16のいずれの方法によっても、図2で示した場合と同様のビット順入れ換えが可能になる。

【0079】図17は、本発明の第3の実施例であるマイクロプロセッサシステムMS3を示す図である。

【0080】マイクロプロセッサシステムMS3は、4つのビット順入れ換えブロック31、32、33、34を有する。つまり、マイクロプロセッサ42の内部にビット順入れ換えブロック31が設けられ、マイクロプロセッサ42のデータバス端子42tとデータバス20との間にビット順入れ換えブロック32が設けられ、データバス20とメモリ11のデータバス端子11tとの間にビット順入れ換えブロック33が設けられ、メモリ11の内部にビット順入れ換えブロック34が設けられている。

【0081】図18は、マイクロプロセッサシステムMS3におけるビット順の入れ換えをより具体的に示す図である。

【0082】ビット順入れ換えブロック31～34にお

いて、それぞれ個別にビット順を入れ換え、マイクロプロセッサコア42cのデータバス端子42cとメモリコア11cのデータバス端子11cとの間で、最終的に、図2に示すビット順の入れ換えと同様のビット順の入れ換えを行っている。

【0083】ここで、ビット順入れ換えブロック31～34のそれぞれの構成として、ビット順入れ換えブロック30、30aの構成を採用してもよく、また、各種ビット順を入れ換える他の構成を採用するようにしてもよい。

【0084】また、マイクロプロセッサシステムMS3において、4つのビット順入れ換えブロック31～34のうちで、少なくとも1つのビット順入れ換えブロックを使用するようにしてもよい。この場合、各ブロック内の入れ換えを適切にすることによって、任意の入れ換えが可能になる。ただし、ビット順入れ換えブロック33のみで構成した場合、またはビット順入れ換えブロック34のみで構成した場合、またはビット順入れ換えブロック33と34とで構成した場合、データバス20上におけるデータは、ビット順が正しく並べ替えられたデータになるので、メモリ11内のデータ観測を阻止することができるが、データバス20を観測されると、正しいプログラムを読み出されてしまう。

【0085】

【発明の効果】本発明によれば、メモリの内容またはデータバス上のデータを読み取られたとしても、第三者がプログラムを解析することが困難であり、ICカード等のプロセッサのセキュリティを向上させることができるという効果を奏する。

【図面の簡単な説明】

【図1】本発明の第1の実施例であるマイクロプロセッサシステムMS1を示す図である。

【図2】上記実施例中のビット順入れ換えブロック30の具体例を示す図である。

【図3】上記実施例におけるメモリ10に格納すべきデータの例を示す図である。

【図4】上記実施例において、メモリ10のデータバス端子10tにおけるプログラムのビット順と、マイクロプロセッサ40のデータバス端子40tにおけるプログラムのビット順とが、どのように変換されているかを具体的に示す図である。

【図5】上記実施例中のビット順入れ換えブロック30の具体例を示す図である。

【図6】ビット順入れ換えブロック30の代わりに使用することができるビット順入れ換えブロック30aの構成を示す図である。

【図7】ビット順入れ換えブロック30aに使用されている各MOSトランジスタの制御信号が、メモリ10に格納されている例を示す図である。

【図8】ビット順入れ換えブロック30aを使用し、図

2に示したビット順の入れ換えをするために、ビット順入れ換えブロック30aに供給する制御信号を示す図である。

【図9】図7に示すトランジスタの制御信号を使用し、ビット順入れ換えブロック30aを制御する場合に必要なメモリセルMCの具体例と、メモリセルMCとトランジスタとの接続関係を示す図である。

【図10】上記実施例において、メモリ10に格納されるビット順変換プログラムの作成法の一例を示す図である。

【図11】上記実施例において、ビット順変換プログラムPによるビット順変換動作を示すフローチャートである。

【図12】本発明の第2の実施例であるマイクロプロセッサシステムMS2を示す図である。

【図13】マイクロプロセッサシステムMS2に使用されているビット順入れ換えブロック30の具体例を示す図である。

【図14】従来のマイクロプロセッサの内部におけるマイクロプロセッサコアと双方向バッファとを示す図である。

【図15】図14に示すマイクロプロセッサ41において、図13に示す実施例を実現する具体的な回路を示す図である。

【図16】図14に示すマイクロプロセッサ41において、図13に示す実施例を実現する別の具体的な回路を示す図である。

【図17】本発明の第3の実施例であるマイクロプロセッサシステムMS3を示す図である。

【図18】マイクロプロセッサシステムMS3におけるビット順の入れ換えをより具体的に示す図である。

【図19】従来のマイクロプロセッサシステムMSの構成の一例を示す図である。

【図20】上記従来例におけるマイクロプロセッサのデータバス端子とメモリのデータバス端子との接続を示す図である。

【図21】上記従来例におけるメモリ1の内容を示す図である。

【符号の説明】

MS1～MS3…マイクロプロセッサシステム、

10…メモリ、

10t…メモリのデータバス端子、

20…データバス、

30、31a、31、32、33、34…ビット順入れ換えブロック、

40、41、42…マイクロプロセッサ、

40t、41t、42t…マイクロプロセッサのデータバス端子、

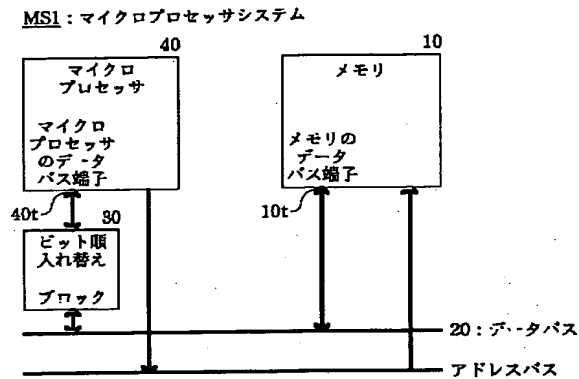
41c、42c…マイクロプロセッサコア、

P…ビット順変換プログラム、

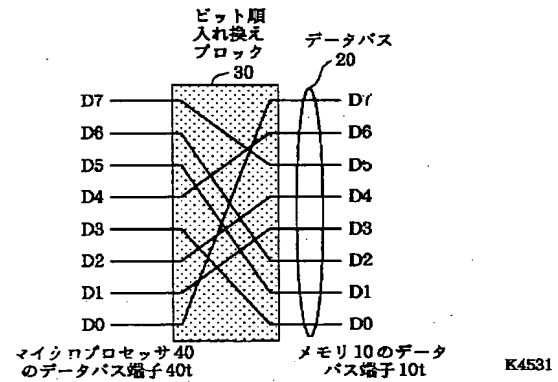
P1...ビット順変換前のプログラム、

P2...ビット順変換後のプログラム。

【図1】



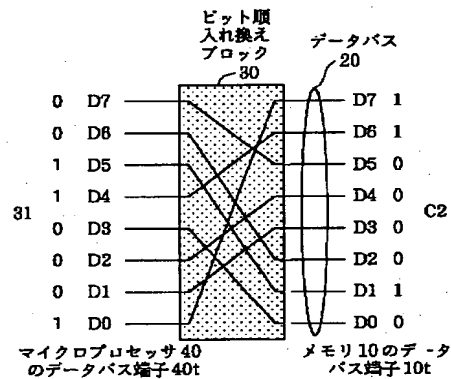
【図2】



【図3】

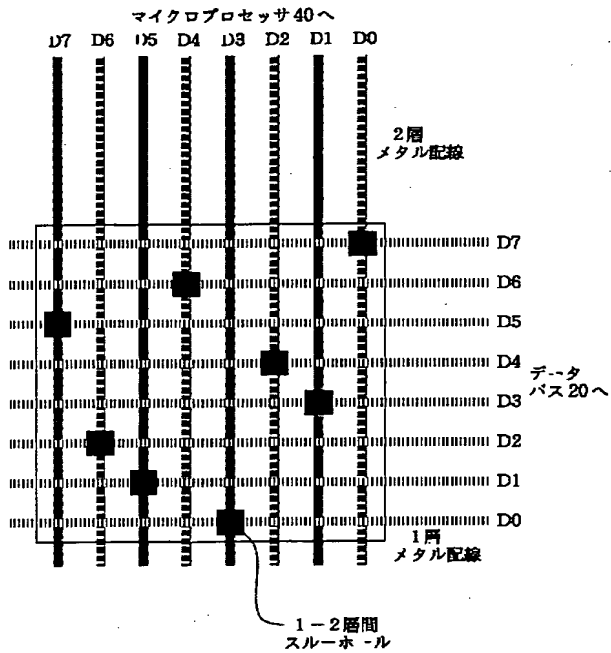
...	...	
9	F4(11110100)	POP BC
8	B4(10110100)	PUSH BC
7	88(10001000)	INC BC
6	0A(00001010)	
5	19(00011001)	LD C, 22
4	C0(11000000)	
3	18(00011000)	LD B, 11
2	DF(11011111)	
1	FF(11111111)	
0	C2(11000010)	LD SP, 7FFF
番地	データ(ヘキシ、6、..., 0)	命令

【図4】



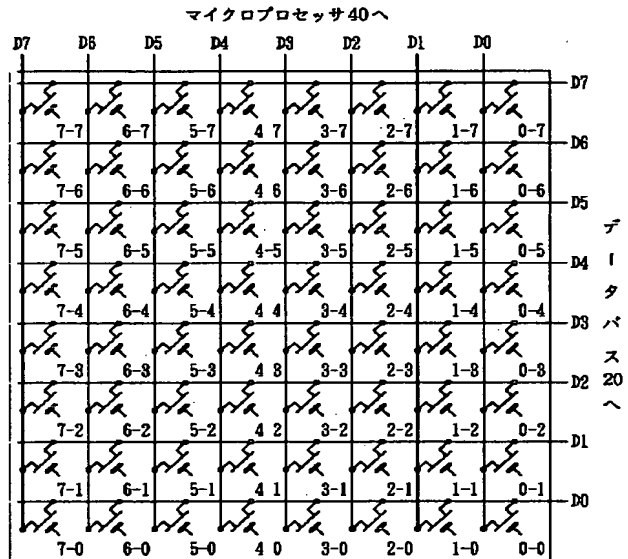
【図5】

30: ビット順入れ換えブロック



【図6】

30a: ビット順入れ換えブロック



K4531

K4531

【図7】

ビット順入れ換えブロック 30aを制御する制御信号

	ビット7							ビット0						
7	7-7	6-7	5-7	4-7	3-7	2-7	1-7	0-7	7	6	5	4	3	2
6	7-6	6-6	5-6	4-6	3-6	2-6	1-6	0-6	6	5	4	3	2	1
5	7-5	6-5	5-5	4-5	3-5	2-5	1-5	0-5	5	4	3	2	1	0
4	7-4	6-4	5-4	4-4	3-4	2-4	1-4	0-4	4	3	2	1	0	
3	7-3	6-3	5-3	4-3	3-3	2-3	1-3	0-3	3	2	1	0		
2	7-2	6-2	5-2	4-2	3-2	2-2	1-2	0-2	2	1	0			
1	7-1	6-1	5-1	4-1	3-1	2-1	1-1	0-1	1	0				
0	7-0	6-0	5-0	4-0	3-0	2-0	1-0	0-0	0					

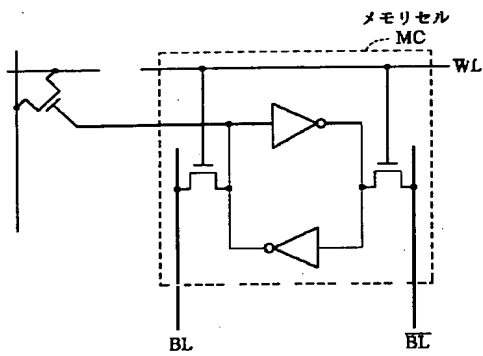
【図8】

ビット順入れ換えブロック 30aを制御する制御信号

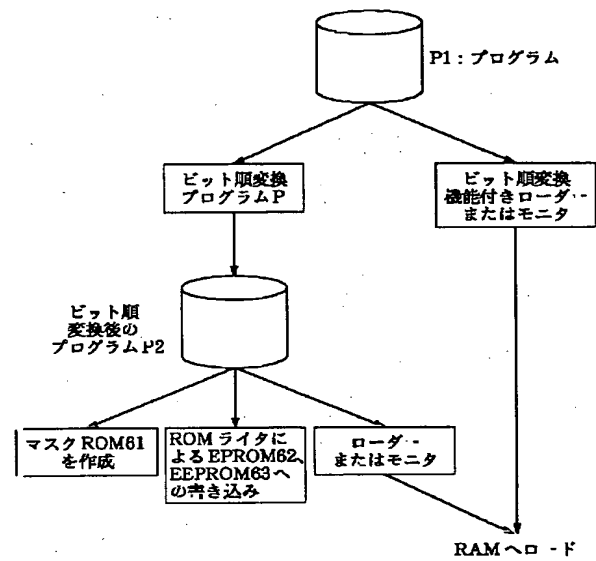
7	00000001
6	00010000
5	10000000
4	00000100
3	00000010
2	01000000
1	00100000
0	00001000

K4531

【図9】



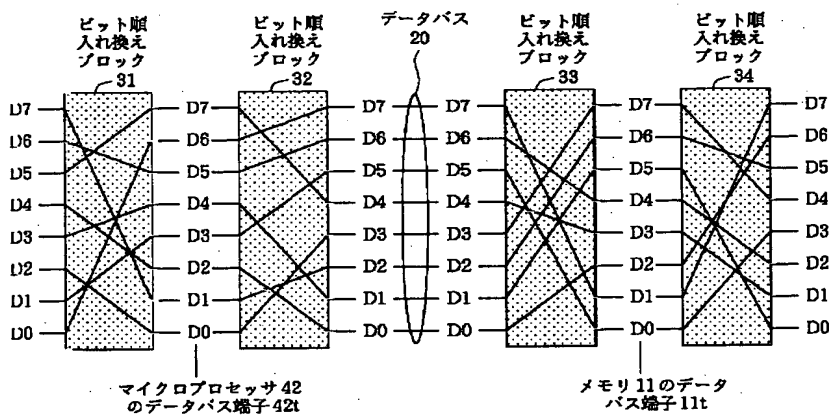
【図10】



K4531

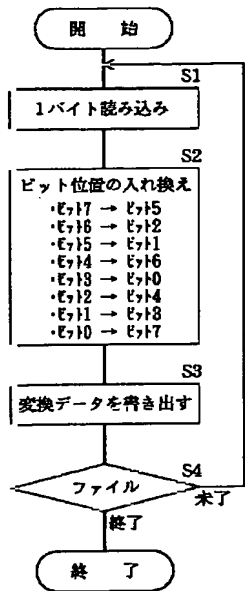
K4531

【図18】



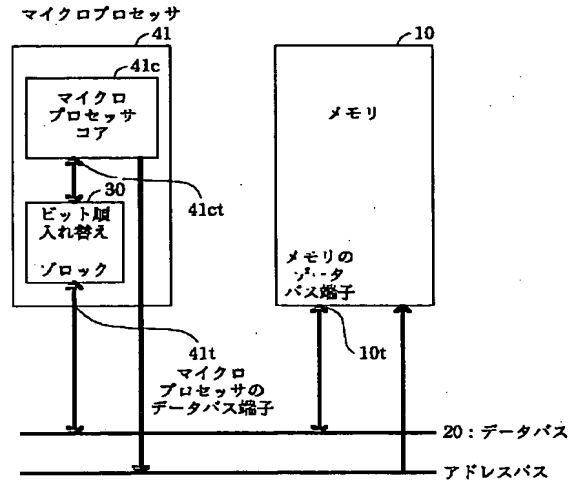
K4531

【図11】



【図12】

MS2: マイクロプロセッサシステム

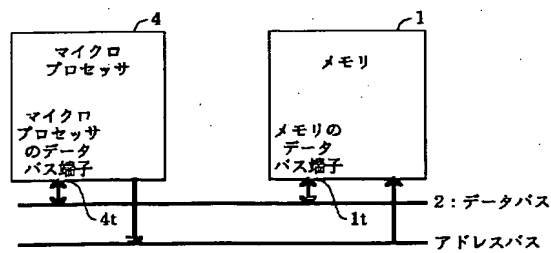


K4531

K4531

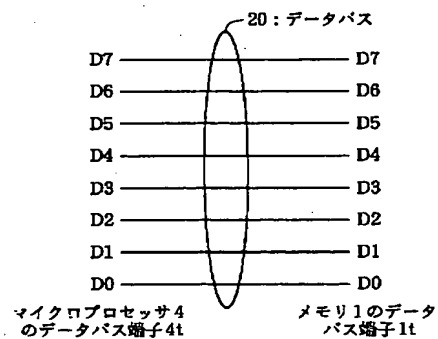
【図19】

MS: マイクロプロセッサシステム



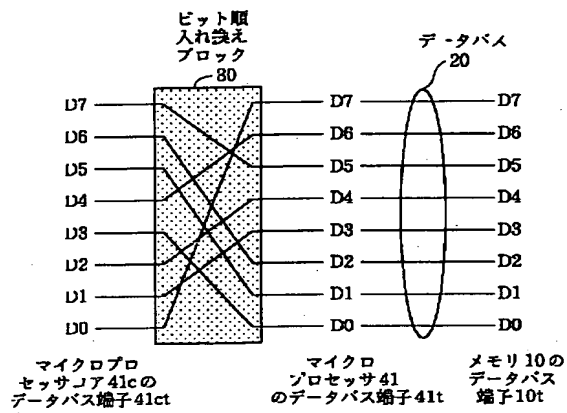
【図20】

メモリ1の内容

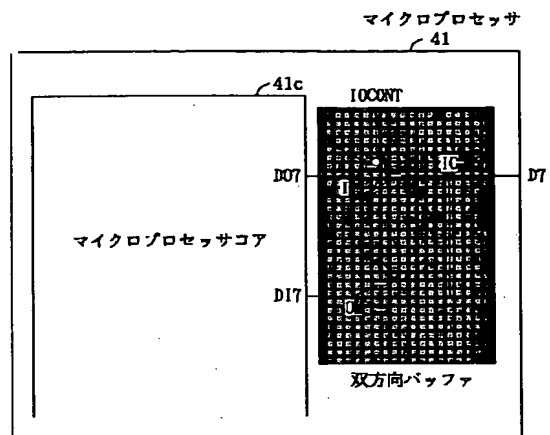


K4531

【図13】



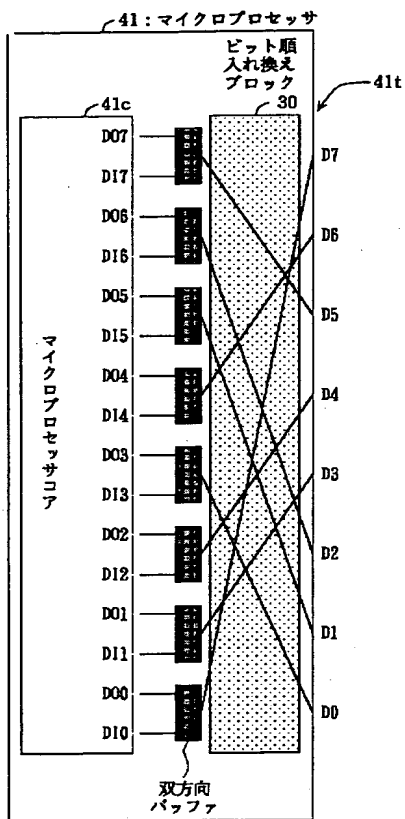
【図14】



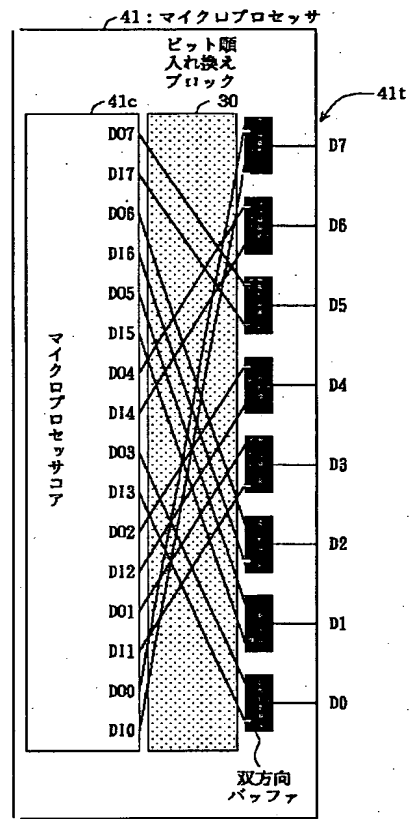
K4531

K4531

【図15】

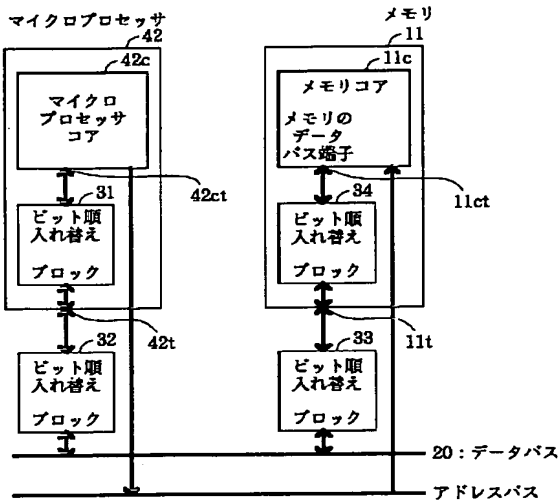


【図16】



【図17】

MS3: マイクロプロセッサシステム



【図21】

メモリ1の内容

...	...	
9	D5(11010101)	POP BC
8	C5(11000101)	PUSH BC
7	03(00000011)	INC BC
6	22(00100010)	
5	0E(00001110)	LD C, 22
4	11(00010001)	
3	06(00000110)	LD B, 11
2	7F(01111111)	
1	FF(11111111)	
0	31(00110001)	LD SP, 7FFF
番地	データ(ビット1, 6, ..., 0)	命令